Congress of the United States
Washington, DC 20515

September 15, 2020

Tim Cook
Chief Executive Officer
Apple
One Apple Park Way
Cupertino, CA 95014

Dear Mr. Cook,

I write to request information from your company regarding the iPhone's feature that wipes phone data after a certain number of failed passcode attempts. I believe this information will be helpful to many Members of Congress and the American public concerned that some members of former Special Counsel Robert Mueller's team may have intentionally wiped their government-issued iPhones, illegally destroying government records in the process.

In response to a Freedom of Information Act (FOIA) request made by Judicial Watch, the Department of Justice (DOJ) has publicly released documents which indicate that several attorneys and staff working on Special Counsel Mueller's team wiped the entirety of data (including emails, text messages, pictures, and call data) on their government-issued iPhones shortly before many of the phones were scheduled to be turned in. From the events described in the DOJ-released documents, it seems to be no coincidence that so many of Mueller's staff members' iPhones were wiped due to a forgotten passcode right before turning them in. If my instinct is correct – that these individuals intentionally subverted potential efforts to investigate their actions during the Mueller investigation – it leads inquiring minds to wonder: what evidence was so damning that they felt the need to destroy it?

Adding to my concerns about the recently released documents is the fact that many members of Mueller's team whose phones were wiped prior to their return blamed the data destruction on an iPhone feature that automatically wipes a phone's data after the wrong passcode is entered consecutively a certain number of times. It is my hope that your company can shed light on this mechanism and how it may have played a role in this case.

To provide some background, of the at least 27 iPhones that were reported to be wiped of their data in the DOJ-released documents, over a dozen of these were reported as iPhones being wiped "on accident" because the phone's user entered their passcode incorrectly too many times. The several such incidents included in the DOJ-released documents secured by a Judicial Watch FOIA request would suggest that it is a common occurrence for a user to accidentally wipe his or her entire iPhone data due to an incorrect passcode. It would be truly shocking if the attorneys chosen to investigate the President of United States – arguably the Democrats' "best and brightest" lawyers – could manage to inadvertently wipe their government-issued iPhones because they spent hours entering an incorrect passcode to a phone they had used for over a year.

It is my understanding that this security feature is intended to prevent unauthorized access via passcode guesses in the event that an iPhone is lost or stolen and includes features to prevent accidental destruction of the data by the user. In fact, widely available information indicates that it would take a minimum of 10 successive incorrect passcodes entered over the course of at least three hours for this security feature to be triggered.

In light of this concerning situation, I request that Apple provide information about this security feature and its history that might improve the understanding of Members of Congress and the American public as to whether the purportedly "accidental" wipes of iPhone data claimed by Andrew Weismann and others on Special Counsel Mueller's staff is as common as they would lead us to believe or if such a widespread technical "mishap" resulting in the triggering of this feature signals it was intentionally manipulated to erase government records. Specifically,

1. For the iPhone 6 and iPhone 7, what is the minimum number of successive failed passcode attempts necessary to trigger the complete destruction of data on an iPhone? Would any data be recoverable via the iPhone itself or through iCloud?
2. For the iPhone 6 and iPhone 7, what is the minimum amount of time that could pass from the first input of an incorrect passcode to the triggering of this security feature, given that the user immediately entered an incorrect passcode as soon as the iPhone unlocked from a previous incorrect attempt?
3. Does your company keep statistics on the reliance of your users on Apple's security features, including the one at issue here? If so, what percentage of iPhone users, outside of iPhones reported lost and/or stolen, do you estimate have accidentally or intentionally wiped their iPhones as a result of this security feature? How many lost or stolen iPhones have been wiped as a result of this security feature?
4. In creating this security feature, was it the goal of your company to minimize the likelihood that a user would accidentally trigger the destruction of data this feature ultimately leads to?

I appreciate your attention to this matter and your prompt response to the questions above.

Sincerely,

Doug Cl

Doug Collins
Member of Congress